LEGALITAS REKAYASA BALIK PROGRAM KOMPUTER DALAM RANGKA PEMBUATAN PROGRAM KEYGEN BERDASARKAN HUKUM POSITIF DI INDONESIA

JURNAL ILMIAH
Untuk Memenuhi Sebagian Syarat-Syarat
Untuk Memperoleh Gelar Kesarjanaan
Dalam Ilmu Hukum

Oleh :
David Omri Sintong
0610113055

DEPARTEMEN PENDIDIKAN NASIONAL
FAKULTAS HUKUM
UNIVERSITAS BRAWIJAYA
MALANG
2014

LEGALITAS REKAYASA BALIK PROGRAM KOMPUTER DALAM RANGKA PEMBUATAN PROGRAM KEYGEN BERDASARKAN HUKUM POSITIF DI INDONESIA

DAVID OMRI SINTONG
Fakultas Hukum Universitas Brawijaya
Email: omri.sitohang@gmail.com

ABSTRAKSI

Rekayasa balik program komputer adalah metode yang dilakukan untuk memperoleh ide atau konsep bekerjanya program komputer yang merupakan obyek yang dilindungi Hak Cipta. Namun, hak Cipta tidak memberikan perlindungan kepada ide atau konsep. Metode rekayasa balik dapat menemukan konsep perlindungan program komputer yang kemudian digunakan untuk membuat program keygen untuk menjebol perlindungan program komputer tersebut. Sehingga dipandang perlu untuk menganalisis legalitas rekayasa balik program komputer khususnya yang dilakukan dalam rangka pembuatan program keygen berdasarkan hukum positif di Indonesia.

Berdasarkan hal tersebut, skripsi ini mengangkat permasalahan: Bagaimana legalitas rekayasa balik program komputer dalam rangka pembuatan program keygen berdasarkan hukum positif di Indonesia? Penulisan bersifat yuridis normatif yaitu penelitian hukum yang dilakukan berdasarkan norma dan kaidah dari peraturan perundangan.

Jawaban dari permasalahan tersebut adalah bahwa rekayasa balik yang dilakukan dalam rangka pembuatan program keygen termasuk perbuatan yang dilarang dalam pasal 30 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (UU ITE) dikarenakan dapat dikatakan sebagai akses ke dalam sistem komputer yang dilakukan untuk memperoleh informasi elektronik berupa kode akses. Keygen yang dibuat setelah rekayasa balik tersebut juga bukan ciptaan yang dilindungi dalam Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta (UUHC), dan kepemilikan keygen tanpa hak juga merupakan pelanggaran hukum dalam UU ITE.

Kata kunci: Rekayasa Balik, Program Komputer, Keygen, Hukum Positif Indonesia

ABSTRACT

Reverse engineering of computer programs is a method to obtain an idea or concept of a computer program which are protected under copyright law. However, copyright does not give protection to idea or concept. Reverse engineering can be used to find the concept of computer programs protection then

used it to create a keygen to break the protection. So it is necessary to analyze the legality of reverse engineering of computer programs specifically in order to make a keygen in terms of positive law in Indonesia .

This thesis attempts to answer: How the legality of reverse engineering of computer programs in order to make a keygen in terms of positive law in Indonesia? This thesis is a normative legal research focusing on the norms and principles of the rule of law.

The answer of the problem is, reverse engineering that's done in order to make a keygen is a prohibited act under section 30 UU ITE because it can be considered as access to computer system to obtain electronic information (access code). Keygen that made after reverse engineering, are not protected under UUHC, and an ownership of keygen also unlawful under UU ITE.

Keywords: Reverse Engineering, Computer Programs, Keygen, key generator, Indonesia Positive Law

A. Pendahuluan

Hak Cipta mengenai program komputer diatur dalam UU No. 19 Tahun 2002 tentang Hak Cipta (untuk penulisan selanjutnya digunakan istilah UUHC). Perlindungan hak cipta program komputer didasarkan pada pemikiran bahwa program komputer merupakan karya cipta di bidang ilmu pengetahuan dan semakin pentingnya peranan dan penggunaan komputer di Indonesia.[1]

Penggunaan *serial number* atau nomor serial produk adalah umum digunakan untuk menghindari pembajakan program komputer.

Cara yang digunakan untuk memodifikasi program komputer untuk membuang (*remove*) dan juga menonaktifkan (*disable*) fitur yang tidak diinginkan biasa disebut dengan istilah *software cracking*. Biasanya fitur-fitur tersebut seperti *copy protection*, *trial* atau *demo version*, *serial number* (nomor serial), *hardware key*, *date check* (untuk *shareware* atau

[1] Karjono, *Perjanjian Lisensi Pengalihan Hak Cipta Program Komputer Transaksi Elektronik* (Bandung: PT Alumni, 2012), hlm 208-209.

demoware), *media CD check*, dan juga berbagai atribut lainnya yang dirasakan mengganggu seperti *Nag Screen/Nagware* dan *Adware*.[2]

Keygen (*key generator*) merupakan sebuah program komputer yang dibuat untuk menghasilkan nomor serial dari program komputer lain yang diproteksi dengan nomor serial.[3]

Rekayasa balik atau *Reverse engineering* (untuk penulisan selanjutnya akan menggunakan istilah Rekayasa balik) adalah proses secara umum untuk menganalisis teknologi, khususnya untuk memastikan bagaimana itu dirancang atau bagaimana beroperasi.[4]

Sebenarnya rekayasa balik memiliki tujuan untuk membuat program menjadi lebih baik karena digunakan untuk menganalisa program tersebut. Rekayasa balik digunakan oleh programer (pembuat program komputer) untuk menganalisis kesalahan yang ada pada program komputer yang sedang dikembangkannya. Sedang seorang *cracker* melakukannya untuk mengetahui kelemahan proteksinya.[5]

Pada penelitian terdahulu dikatakan [6] bahwa rekayasa balik program komputer bukan suatu pelanggaran Hak Cipta dikarenakan rekayasa balik merupakan upaya untuk mendapatkan ide atau konsep dari suatu program komputer. Ide atau konsep tidak dilindungi oleh hak cipta. Penelitian lain juga mengatakan bahwa rekayasa balik termasuk *fair use* (penggunaan yang wajar).[7][8]

Rekayasa balik juga bukan suatu pelanggaran rahasia dagang apabila informasi rahasia melekat pada sebuah produk sedemikian rupa

---

2 Feri Sulianta, *Software Cracking*, (Jakarta: PT. Elex Media Komputindo, 2010), hlm 1

3 Yessah Ihut Adam, *Software Cracking Dengan Reverse Engineering*, Penulisan Ilmiah, 2010, hlm 24.

4 Eldad Eilam, *Reversing: Secrets of Reverse Engineering* (Indianapolis: Wiley Publishing, 2005),.hlm 3-4.

5 Yessah Ihut Adam, *Op.Cit.*, hlm 5.

6 Afifah Kusumandara, *Perlindungan Program Komputer Menurut Hukum Hak Kekayaan Intelektual*. Jurnal Hukum dan Pembangunan, No. 3, 2003, hlm 4.

7 Ariyanti. *Reverse Engineering Program Komputer Dalam Perspektif Hukum Hak Cipta dan Paten di Indonesia dan Malaysia*, Tesis, 2009. hlm 100

8 Yourdha Triyudanto, *Analisis Terhadap Rekayasa Balik Program Komputer Metode Jailbreak; Tinjauan dari Hukum Hak Cipta*, Tesis, 2012, hlm 91

sehingga memungkinkan pihak lain mempelajari, menelaah dan menganalisis rahasia tersebut.[9] [10]

Disinilah muncul permasalahan dikarenakan informasi yang didapatkan dari proses rekayasa balik dapat berupa ide atau konsep proteksi, seperti algoritma atau kombinasi nomor serial (*serial number*), sehingga diketahui bagaimana nomor serial yang *valid* yang dapat digunakan untuk membuka proteksinya.

Dengan mendapatkan pengetahuan proteksi program komputer berupa algoritma atau kombinasi nomor serial, seseorang dapat membuat program baru, yakni program keygen (*key generator*), yang fungsinya hanya untuk menghasilkan kombinasi nomor serial program komputer yang diproteksi.

Program Keygen merupakan program komputer yang dibuat untuk menghasilkan nomor serial program komputer lain. Seperti yang telah dijelaskan sebelumnya, program komputer merupakan karya cipta yang dilindungi, seperti yang diatur dalam pasal 12 ayat (1) huruf a Undang-Undang Hak Cipta.

Oleh karena itu sangat penting untuk menganalisis lebih lanjut tentang pengaturan mengenai program komputer dalam hukum positif di Indonesia khususnya yang berkaitan dengan rekayasa balik, terutama yang bertujuan untuk pembuatan program keygen.

B. Permasalahan

Berdasarkan latar belakang yang telah dijelaskan diatas, peneliti merumuskan beberapa masalah pokok yang menjadi ruang lingkup penulisan skripsi sebagai berikut:

---

[9] Lucky Setiawati, *Rahasia Dagang dan Perlindungan Formula Resep Makanan*, http://www.hukumonline.com/klinik/detail/lt4feadb7627be1/rahasia-dagang-dan-perlindungan-formula-resep-makanan, diakses pada 25 januari 2014.

[10] Harry Agustanto, *Perlindungan Kerahasiaan Source Code pada Program Komputer*, Tesis, 2011, hlm 98

Bagaimana legalitas rekayasa balik program komputer yang bertujuan untuk pembuatan program keygen berdasarkan hukum positif di Indonesia?

C. Metode Penelitian

Penelitian ini menggunakan metode pendekatan Yuridis Normatif. Dalam penelitian atau pengkajian ilmu hukum normatif, kegiatan untuk menjelaskan hukum tidak diperlukan dukungan data atau fakta-fakta sosial, sebab ilmu hukum normatif tidak mengenal data atau fakta sosial, yang dikenal hanya bahan hukum. Jadi untuk menjelaskan hukum atau untuk mencari makna dan memberi nilai akan hukum tersebut hanya digunakan konsep hukum dan langkah-langkah yang ditempuh adalah langkah normatif.[11]

D. Bahan-Bahan Hukum

1. Bahan hukum primer, yaitu bahan-bahan hukum yang mengikat[12] yakni undang-undang yang berkaitan dengan Hak Kekayaan Intelektual dan program dan pengguna komputer. Antara lain:
    a. Pasal 3 ayat (1), Pasal 14, dan Pasal 15 huruf b Undang-undang Nomor 30 Tahun 2000 Tentang Rahasia Dagang
    b. Pasal 1 angka 8, Pasal 12 ayat (1) huruf a, pasal 15, dan pasal 27 Undang-undang Nomor 19 Tahun 2002 Tentang Hak Cipta.
    c. Pasal 1 butir 1, 15 dan 16, pasal 30 ayat (2) dan (3), pasal 34 ayat (1) huruf a dan b Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
    d. Pasal 22 ayat (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
2. Bahan hukum sekunder, yaitu bahan-bahan yang erat hubungannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami

---

[11] Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum,* (Bandung: Mandar Maju, 2008), hlm 87.

[12] Muslan Abdurrahman, *Sosiologi dan metode penelitian hukum* (Malang: UMM Press, 2009), hlm 127.

bahan hukum primer[13], yakni bersumber dari pendapat para ahli dan buku-buku termasuk skripsi, tesis, disertasi dan jurnal[14] di bidang rekayasa perangkat lunak dan hak kekayaan intelektual.

3. Bahan hukum tersier, yaitu bahan yang digunakan untuk memahami bahan primer dan sekunder, seperti kamus dan ensiklopedia, serta literatur mengenai bidang diluar hukum yang terkait dengan pembahasan penelitian.

E. Tehnik Pengumpulan Bahan Hukum

Tehnik pengumpulan bahan hukum yakni dengan *library research* atau studi pustaka yang dilakukan dengan melakukan penelusuran bahan hukum dengan mempelajari peraturan perundang-undangan dan literatur lainnya seperti jurnal, karya ilmiah, dan buku sehingga dapat diperoleh informasi untuk mengkaji topik permasalahan.

F. Teknik Analisis Bahan Hukum

Teknik analisis bahan hukum menggunakan interpretasi dan logika deduksi sebagai teknik analisis bahan hukum dalam penelitian ini. Interpretasi atau penafsiran merupakan salah satu metode penemuan hukum yang memberikan penjelasan yang gamblang mengenai teks undang-undang agar ruang lingkup kaidah dapat ditetapkan sehubungan dengan peristiwa tertentu.[15]

G. Pembahasan

Program komputer sebagai bagian dari teknologi komputer merupakan karya cipta yang dilindungi dalam Pasal 12 ayat (1) huruf a UUHC:

> Dalam Undang-undang ini Ciptaan yang dilindungi adalah Ciptaan dalam bidang ilmu pengetahuan, seni, dan sastra, yang mencakup:

---

13 *Ibid.*

14 Peter Mahmudi Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2005), hlm 155.

15 Sudikno Mertokusumo, *Mengenal Hukum (Suatu Pengantar).* (Yogyakarta: Liberty, 2003), hlm 170.

a. buku, Program Komputer, pamflet, perwajahan (layout) karya tulis yang diterbitkan, dan semua hasil karya tulis lain;

Definisi program komputer terdapat dalam Pasal 1 angka 8 UUHC dan penjelasan umum UU ITE, yakni:

> Sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi-instruksi tersebut.

Untuk melindungi program komputer dari pembajakan, biasanya pengembang program komputer melengkapi programnya dengan sarana kontrol teknologi.

Penjelasan pasal 27 UUHC menjelaskan yang dimaksud dengan Sarana Kontrol Teknologi adalah

> instrumen teknologi dalam bentuk antara lain kode rahasia, password, bar code, serial number, teknologi dekripsi (decryption) dan enkripsi (encryption) yang digunakan untuk melindungi Ciptaan.

Hak Cipta terdiri atas hak ekonomi (*economic rights*) dan hak moral (*moral rights*). Hak ekonomi adalah hak untuk mendapatkan manfaat ekonomi atas Ciptaan serta produk Hak Terkait. Dapat dikatakan sarana kontrol teknologi berfungsi sebagai perlindungan hak pencipta termasuk yang berupa hak ekonomi.

Pengaturan mengenai sarana kontrol teknologi terdapat dalam pasal 27 UUHC yang menyatakan:

> "kecuali atas izin Pencipta, sarana kontrol teknologi sebagai pengaman hak pencipta tidak diperbolehkan dirusak, ditiadakan, atau dibuat tidak berfungsi."

Penerapan sarana kontrol teknologi juga terdapat dalam PP-STE. Pasal 22 ayat (2) PP-STE mengatur:

> dalam penyelenggaraan Sistem Elektronik yang ditujukan untuk Informasi Elektronik dan/atau Dokumen Elektronik yang dapat dipindahtangankan, Informasi Elektronik dan/atau Dokumen Elektronik harus unik serta menjelaskan penguasaan dan kepemilikannya.

Yang dimaksud dengan "Informasi Elektronik dan/atau Dokumen Elektronik harus menjelaskan kepemilikan" adalah:[16]

> ...Informasi Elektronik dan/atau Dokumen Elektronik tersebut harus menjelaskan sifat kepemilikan yang direpresentasikan oleh adanya sarana kontrol teknologi yang menjamin hanya ada satu salinan yang sah (*single authoritative copy*) dan tidak berubah.

Jika dikaitkan antara pasal 27 UUHC dengan pasal 22 PP-STE, dapat menjelaskan fungsi lain dari sarana kontrol teknologi, yakni untuk menjelaskan pengguna yang sah dari program komputer. Contoh penggunaan sarana kontrol teknologi adalah program komputer yang dilindungi nomor serial *(serial number)* atau kode akses. Nomor serial atau kode akses digunakan oleh program komputer untuk mengidentifikasi pengguna yang sah dan berhak untuk menggunakan program tersebut.

Sarana kontrol teknologi pada program komputer yang umum digunakan adalah perlindungan dengan nomor serial. Pengembang perangkat lunak mengirimkan tiap salinan program dengan mencetak nomor serial yang unik di suatu tempat di kemasan produk atau di medianya. Instalasi program kemudian meminta pengguna untuk menuliskan nomor tersebut pada saat proses instalasi. Program instalasi mencocokan apakah nomor yang dimasukan valid (dengan menggunakan algoritma validasi rahasia), dan jika valid, program akan terinstal dan terdaftar pada sistem pengguna.

---

[16] Lihat penjelasan pasal 22 ayat (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Proses instalasi biasanya menambahkan nomor serial atau suatu turunannya dalam informasi pendaftaran pengguna. Sehingga jika pengguna menghubungi *customer support* (layanan konsumen), pengembang program komputer dapat melakukan verifikasi bahwa pengguna memiliki instalasi produk yang valid.[17]

Cara untuk menjebol atau melewati sarana kontrol teknologi, salah satunya adalah melalui rekayasa balik. Rekayasa balik adalah proses menganalisa sebuah program komputer untuk merepresentasikan program tersebut ke informasi pada level yang lebih dalam, bisa juga dikatakan menganalisa sebuah sistem seperti pada saat sistem tersebut sedang dikembangkan.[18]

Konsep Rekayasa balik yang diterapkan pada program komputer biasanya mengacu pada praktik yang dilakukan untuk memahami bagaimana program tersebut dibangun dan bagaimana program tersebut mencapai fungsionalitasnya.[19]

Proses rekayasa balik dilakukan dengan adanya beberapa program komputer pendukung, diantaranya adalah *Disassembler*, *Debugger*, dan *Decompiler*.

Disassembler adalah program yang dibuat untuk membuka sebuah *executable binary* sebagai input dan menghasilkan kode assembler dari *executable binary* tersebut sebagai output. *Debugger* adalah program yang dibuat untuk menganalisa sebuah program lain pada saat program itu berjalan. Sedangkan *decompiler* merupakan perkembangan dari disassembler. *Decompiler* digunakan untuk memproduksi kode dari *executable binary* menjadi mirip dari kode sumber program tersebut atau sedikit banyak menjadi mirip kode sumber program tersebut.

---

17 Eldad Eilam, *Op.Cit.*, hlm 3, terjemahan bebas.

18 Yessah Ihut Adam, *Op.Cit.*, hlm 5.

19 Robert H. Lande. Harvard Journal of Law and Technology, Volume 9, Number 2 Summer 1996, hlm 240, terjemahan bebas.

Sesungguhnya memproduksi kode asli dari sebuah *executable binary* merupakan hal yang sangat mustahil.[20]

Rekayasa balik juga dapat digunakan untuk menganalisis dan akhirnya untuk mengalahkan berbagai skema perlindungan salinan seperti sarana kontrol teknologi.

Rekayasa balik tidak dilarang dalam UUHC dikarenakan rekayasa balik bertujuan untuk memperoleh ide atau konsep yang bukan merupakan obyek yang dilindungi UUHC. Namun dikarenakan rekayasa balik tersebut dapat dikatakan sebagai akses terhadap sistem elektronik, maka rekayasa balik yang dilakukan sebagai upaya untuk mendapatkan informasi elektronik, yakni berupa kode akses atau nomor serial termasuk perbuatan yang dilarang dalam pasal 30 ayat (2) UU ITE:

> (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Sanksi terhadap pelanggaran pasal 30 ayat (2) UU ITE terdapat dalam pasal 46 ayat (2) UU ITE:

> (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

Pasal 30 ayat (3) UU ITE juga melarang:

> (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pada penjelasan pasal 30 ayat (3) yang dimaksud dengan sistem pengaman adalah sistem yang membatasi akses Komputer atau melarang

[20] Yessah Ihut Adam. *Op.Cit.*

akses ke dalam Komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

Sistem pengaman dalam UU ITE memiliki persamaan dengan sarana kontrol teknologi dalam UUHC, yakni untuk menjelaskan pengguna yang sah. Atau, dengan kata lain, hak dari pengguna terhadap akses.

Dikarenakan hal itu, maka penggunaan kode akses tanpa hak yang dilakukan untuk mengakses program komputer juga termasuk perbuatan yang dilarang dalam pasal 30 ayat (3) UU ITE. Sanksi terhadap perbuatan tersebut terdapat dalam pasal 46 ayat (3) UU ITE:

> (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Keygen yang dibuat berdasarkan hasil rekayasa balik tersebut, juga kode akses yang dihasilkannya, adalah dilarang kepemilikannya dalam pasal 34 ayat (1) huruf a dan b UU ITE:

> (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
>
> a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
>
> b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Sanksi terhadap kepemilikan keygen terdapat dalam pasal 50 UU ITE:

> Pasal 50

> Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah).

Program yang dilarang hanyalah program yang dikembangkan secara khusus untuk perbuatan yang dilarang dalam pasal 27 sampai dengan pasal 33 UU ITE. Program yang digunakan untuk rekayasa balik seperti debugger, disassembler, atau decompiler tidak termasuk yang dilarang dikarenakan dapat digunakan untuk kegiatan selain untuk tujuan yang dilarang.

Seperti ketentuan dalam pasal 27 UUHC bahwa Sarana Kontrol Teknologi tidak diperbolehkan dirusak, ditiadakan, atau dibuat tidak berfungsi. Dapat dikatakan, sarana kontrol teknologi tidak berfungsi untuk menjelaskan pengguna yang sah dari program komputer jika seseorang secara tidak sah memperoleh nomor serial untuk mengakses program komputer dan dapat dikatakan sebagai pelanggaran terhadap sarana kontrol teknologi.

Sanksi terhadap pelanggaran pasal 27 UUHC terdapat pada pasal 72 UUHC ayat (8):

> (8) Barangsiapa dengan sengaja dan tanpa hak melanggar Pasal 27 dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 150.000.000,00 (seratus lima puluh juta rupiah).

Pada penelitian sebelumnya dijelaskan bahwa rekayasa balik tidak dilarang karena termasuk *fair use* atau penggunaan yang wajar dikarenakan ciptaan baru memenuhi unsur originalitas. [21] Rekayasa balik juga dapat dikatakan sebagai penggunaan yang wajar, selama tidak bersifat komersial, dikarenakan rekayasa balik adalah upaya untuk memperoleh akses atas ilmu pengetahuan.[22]

---

21 Ariyanti, *Op.Cit.*.

22 Yourdha Triyudanto, *Op.Cit.*

Black's Dictionary mendefinisikan *Fair use* atau penggunaan yang wajar sebagai:

> "*A reasonable and limited use of copyrighted work without the author's permission, such as quoting from a book in a book review, or using parts of it in a parody. Fair use is a defense to an infringement claim, depending on the following statutory factors: 1) The purpose and character of the use; 2) The nature of the copyrighted work; 3) The amount of work used; and 4) The economic impact of the use (on the copyright holder).*"

Penjelasan pasal 15 huruf a menjelaskan yang dimaksud dengan "kepentingan yang wajar" yakni:

> "..suatu kepentingan yang didasarkan pada keseimbangan dalam menikmati manfaat ekonomi atas suatu ciptaan."

Rekayasa balik dalam rangka membuat program keygen adalah rekayasa balik yang dilakukan dengan tujuan untuk memperoleh kode akses dapat merugikan kepentingan pencipta atau pembuat program untuk menikmati manfaat ekonomi atas ciptaan, dikarenakan program menjadi dapat digunakan tanpa memerlukan kode akses atau nomor serial yang harus dibeli dari pengembang program. Rekayasa balik yang dilakukan dalam rangka pembuatan program keygen tidak dapat dikatakan sebagai fair use atau penggunaan yang wajar dikarenakan dapat merugikan hak ekonomi dari pencipta.

Rekayasa balik bukanlah perbuatan yang dilarang dalam UUHC namun penggunaan keygen atau kode akses palsu dapat dikatakan sebagai pelanggaran terhadap sarana kontrol teknologi atau hak cipta.

Terkait keygen yang dibuat berdasarkan hasil rekayasa balik, Pasal 17 UUHC menyatakan:

> "Pemerintah melarang Pengumuman setiap Ciptaan yang bertentangan dengan kebijaksanaan Pemerintah di bidang agama,

pertahanan dan keamanan Negara, kesusilaan, serta ketertiban umum setelah mendengar pertimbangan Dewan Hak Cipta."

Tidak terdapat penjelasan apa yang dimaksud dengan "ketertiban umum" dalam UUHC karena penjelasan pasal 17 hanya dinyatakan cukup jelas. Namun dengan menggunakan penafsiran secara sistematis komparatif, yaitu mengambil pengertian "ketertiban umum" dari ketentuan-ketentuan yang lain yang terdapat dalam peraturan perundang-undangan yang memiliki "rumpun" yang sama, yaitu peraturan perundang-undangan yang melingkupi bidang hak kekayaan intelektual, maka pengertian "bertentangan dengan kepentingan umum" dapat ditafsirkan sebagai "beritikad tidak baik", penafsiran ini sesuai dengan Penjelasan Pasal 69 ayat (2) kalimat kedua Undang-Undang Nomor 15 Tahun 2001 tentang Merek, yang berbunyi sebagai berikut: "termasuk pula dalam pengertian yang bertentangan dengan kepentingan umum adalah adanya iktikad tidak baik."[23]

Pengertian itikad baik (*good faith*) menurut Black Law Dictionary adalah:[24]

> "*good faith consists in an honest intention to abstain from taking any unconscientious advantage of another, even through the forms or technicalities of law, together with an absence of all information or belief of facts which would render the transaction unconscientious."*

Itikad tidak baik adalah kebalikan dari itikad baik. Itikad tidak baik (*bad faith*) menurut black law dictionary adalah:[25]

---

23 Lihat pertimbangan Mahkamah Agung mengenai pengertian "bertentangan dengan kepentingan umum" dalam UU Desain Industri.dalam Putusan Mahkamah Agung Nomor : 022 K/N/HaKI/2006.

24 Henry Campbell Black, *Black's Law Dictionary 2nd ed*. (St. Paul, Minn.: West Publishing, 1910), hlm 544.

25 *Ibid*, hlm 112.

"the opposite of "good faith," generally implying or involving actual or constructive fraud, or a design to mislead or deceive another, or a neglect or refusal to fulfill some duty or some contractual obligation, not prompted by an honest mistake as to one's rights or duties, but by some interested or sinister motive."

Keygen yang digunakan untuk mendapatkan nomor serial program komputer tanpa harus membeli program yang asli dapat dianggap sebagai usaha menghindari kewajiban sebagai konsumen. Dengan demikian, jika dilihat dari tujuannya, dapat dikatakan bahwa keygen termasuk ciptaan yang dilarang dalam Pasal 17 UUHC.

Dalam konteks rahasia dagang, algoritma yang dirahasiakan termasuk obyek yang dilindungi dalam UURD. Namun, perlindungan rahasia dagang mensyaratkan harus ada upaya-upaya tertentu yang dilakukan untuk merahasiakannya. Pasal 3 ayat (1) UURD menyebutkan:

> Rahasia Dagang mendapat perlindungan apabila informasi tersebut bersifat rahasia, mempunyai nilai ekonomi, dan dijaga kerahasiaannya melalui upaya sebagaimana mestinya.

Yang dimaksud upaya-upaya sebagaimana mestinya adalah semua langkah yang memuat ukuran kewajaran, kelayakan, dan kepatutan yang harus dilakukan.[26]

Rekayasa balik adalah hal yang lumrah dilakukan dalam proses pengembangan program komputer karena salah satu fungsinya adalah untuk memperbaiki program komputer. Untuk itu harus terdapat upaya tertentu agar algoritma atau konsep program tidak mudah terbaca pada proses rekayasa balik.

Terdapat upaya-upaya untuk melindungi konsep program komputer terhadap rekayasa balik, antara lain enkripsi yang diterapkan pada string atau algoritma.[27]

---

[26] Penjelasan pasal 3 ayat (1) UURD

Kompilasi program komputer, yakni menerjemahkan kode sumber menjadi kode obyek, bukanlah upaya yang khusus dilakukan untuk menjaga kerahasiaan karena tujuan kompilasi sebenarnya adalah agar program dapat dibaca oleh mesin.

Dalam Pasal 14 UURD diatur bahwa:

> Seseorang dianggap melanggar Rahasia Dagang pihak lain apabila ia memperoleh atau menguasai Rahasia Dagang tersebut dengan cara yang bertentangan dengan peraturan perundang-undangan yang berlaku.

Algoritma perlindungan program komputer yang dirahasiakan seperti algoritma sarana kontrol teknologi juga termasuk obyek yang dilindungi oleh UURD. Program Keygen bekerja sesuai dengan algoritma sarana kontrol teknologi program lain. Ini artinya, untuk membuat program keygen maka harus didahului dengan memperoleh pengetahuan mengenai algoritma program lain yang dilindungi rahasia dagang. Jika algoritma tersebut diperoleh dengan cara seperti dalam Pasal 30 ayat (2) UU ITE maka dianggap suatu pelanggaran rahasia dagang.

Sanksi terhadap pelanggaran rahasia dagang terdapat dalam Pasal 17 UURD:

> (1) Barangsiapa dengan sengaja dan tanpa hak menggunakan Rahasia Dagang pihak lain atau melakukan perbuatan sebagaimana dimaksud dalam pasal 13 atau Pasal 14 dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp.300.000.000,00 (tiga ratus juta rupiah).
> (2) Tindak pidana sebagaimana dimaksud dalam ayat (1) merupakan delik aduan.

---

[27] Yessah Ihut Adam. *Op.Cit.*

Penutup

a. Kesimpulan

Berdasarkan pembahasan yang telah diuraikan pada bab sebelumnya, dapat disimpulkan bahwa:

Rekayasa balik yang dilakukan dalam rangka untuk pembuatan program keygen tidak dilarang dalam UUHC dikarenakan tujuannya untuk mendapatkan konsep atau ide yang bukan merupakan obyek yang dilindungi hak cipta. Rekayasa balik yang dilakukan untuk memperoleh rahasia dagang orang lain juga tidak dilarang dalam UURD. Namun, dikarenakan rekayasa balik ini dapat dikatakan sebagai akses kedalam sistem komputer, maka rekayasa balik untuk tujuan tersebut termasuk perbuatan yang dilarang dalam pasal 30 ayat (2) UU ITE dikarenakan tujuannya adalah memperoleh informasi elektronik berupa kode akses secara tanpa hak. Keygen juga termasuk program yang dilarang dalam pasal 34 ayat (1) huruf a UU ITE karena merupakan program yang secara khusus dikembangkan untuk memfasilitasi pelanggaran menurut ketentuan pasal 30 ayat (2) UU ITE. Program yang dilakukan untuk melakukan rekayasa balik seperti *decompiler, debugger*, atau *disassembler* tidak termasuk program yang dilarang dalam pasal 30 ayat (2) UU ITE karena dapat digunakan untuk keperluan lain selain yang dilarang dalam Pasal 27 sampai dengan Pasal 33 UU ITE. Penggunaan keygen dapat merugikan kepentingan ekonomi pencipta sehingga dapat dikatakan sebagai pelanggaran hak cipta dan merupakan pelanggaran terhadap pasal 27 UUHC. Keygen juga merupakan program yang dilarang dalam pasal 17 UUHC sehingga tidak dilindungi hak cipta dikarenakan keygen adalah ciptaan yang termasuk ke dalam unsur

"bertentangan dengan kepentingan umum." Rekayasa balik yang dilakukan untuk mendapatkan rahasia dagang milik orang lain bukan merupakan pelanggaran rahasia dagang, namun dikarenakan rekayasa balik yang khusus dilakukan untuk membuat keygen termasuk perbuatan yang dilarang dalam pasal 30 ayat (2) UU ITE sehingga memenuhi unsur pasal 14 UURD yakni "menguasai Rahasia Dagang tersebut dengan cara yang bertentangan dengan peraturan perundang-undangan yang berlaku" maka rekayasa balik yang dilakukan dalam rangka pembuatan program keygen merupakan pelanggaran rahasia dagang. Sanksi pidana rekayasa balik dalam rangka pembuatan program keygen terdapat pada pasal 46 ayat (2) UU ITE dan Pasal 17 UURD. Sanksi terhadap penggunaan keygen yang dibuat dari rekayasa balik tersebut terdapat pada pasal 46 ayat (3) UU ITE dan pasal 72 ayat (8) UUHC. Sedangkan sanksi pidana kepemilikan keygen terdapat pada Pasal 50 UU ITE.

b. Saran

Berdasarkan temuan yang ada selama penelitian maka disarankan:

1. Bagi pengembang program komputer:

   Rekayasa balik yang dilakukan dengan tujuan untuk memperoleh informasi elektronik berupa kode akses merupakan perbuatan yang dilarang dan harus dihindari. Algoritma program komputer yang dapat terlihat dalam proses rekayasa balik program komputer bukan merupakan obyek yang dilindungi oleh hak cipta dikarenakan algoritma masih berupa ide atau konsep. Algoritma dapat dilindungi rahasia dagang, namun untuk mendapat perlindungan rahasia dagang, pengembang program harus melakukan upaya-upaya merahasiakan algoritma tersebut seperti misalnya melakukan enkripsi pada algoritma. Kompilasi

program komputer, yakni menerjemahkan kode sumber menjadi kode obyek, bukanlah upaya yang khusus dilakukan untuk menjaga kerahasiaan karena tujuan kompilasi sebenarnya adalah agar program dapat dibaca oleh mesin.

2. Bagi masyarakat umum:

   Penggunaan program komputer komersil dengan menggunakan nomor serial atau kode akses ilegal, yakni nomor serial atau kode akses yang didapat secara tanpa hak, merupakan pelanggaran hak cipta dan UU ITE. Kepemilikan keygen dilarang oleh UU ITE. Karena itu disarankan kepada masyarakat untuk menghindari kepemilikan keygen dan penggunaan kode akses yang dihasilkannya.

3. Bagi pembuat undang-undang:

   Rekayasa balik terhadap program komputer belum diatur secara tegas dalam hukum positif di Indonesia. Rekayasa balik terhadap program komputer sangat terkait dengan penggunaan yang wajar dari ciptaan. Sulit untuk menentukan ukuran "penggunaan yang wajar" dalam pasal 15 UUHC. Untuk itu disarankan bagi pembuat Undang-undang untuk memasukan *Berne three-step test* dalam revisi UUHC.

Daftar Pustaka

Buku

Bahder Johan Nasution, **Metode Penelitian Ilmu Hukum**, Mandar Maju, Bandung, 2008.

Eldad Eilam, **Reversing: Secrets of Reverse Engineering**, Wiley Publishing, Indianapolis, 2005.

Feri Sulianta, **Software Cracking**, PT. Elex Media Komputindo, Jakarta, 2010.

Henry Campbell Black, **Black's Law Dictionary 2nd ed**. St. Paul, Minn.: West Publishing, 1910.

Muslan Abdurrahman, **Sosiologi dan Metode Penelitian Hukum**, UMM Press, Malang, 2009.

Karjono, **Perjanjian Lisensi Pengalihan Hak Cipta Program Komputer Transaksi Elektronik**, PT Alumni, Bandung, 2012.

Peter Mahmudi Marzuki, **Penelitian Hukum**, Kencana, Jakarta, 2005.

Sudikno Mertokusumo, **Mengenal Hukum (Suatu Pengantar)**. Liberty, Yogyakarta, 2003.

Karya Ilmiah dan Jurnal

Afifah Kusumandara, **Perlindungan Program Komputer Menurut Hukum Hak Kekayaan Intelektual**. Jurnal Hukum dan Pembangunan, No. 3, Fakultas Hukum Universitas Indonesia, Depok, 2003.

Robert H Lande, **Reverse Engineering of Computer Software and U.S. Antitrust Law**. Harvard Journal of Law and Technology, volume 9, Harvard University, Massachusetts, 1996.

Yessah Ihut Adam. **Software Cracking Dengan Reverse Engineering.** Penulisan Ilmiah. Universitas Gunadarma, Depok, 2010.

Tesis

Ariyanti. **Reverse Engineering Program Komputer Dalam Perspektif Hukum Hak Cipta dan Paten di Indonesia dan Malaysia**, Tesis diterbitkan. Semarang, Fakultas Hukum Universitas Diponegoro, 2009.

Yourdha Triyudanto. **Analisis Terhadap Rekayasa Balik Program Komputer Metode Jailbreak; Tinjauan dari Hukum Hak Cipta**. Tesis diterbitkan. Jakarta, Fakultas Hukum Universitas Indonesia, 2012.

Harry Agustanto. **Perlindungan Kerahasiaan Source Code Pada Software Komputer (Studi Kasus Reverse Engineering)**. Tesis diterbitkan. Jakarta: Universitas Indonesia, 2011.

Internet

Lucky Setiawati. **Rahasia Dagang dan Perlindungan Formula Resep Makanan**, http://www.hukumonline.com/klinik/detail/lt4feadb7627be1/rahasia-dagang-dan-perlindungan-formula-resep-makanan, diakses 24 januari 2014.

Peraturan Perundang-Undangan

Undang-undang Nomor 30 Tahun 2000 tentang Rahasia Dagang
Undang-undang Nomor 19 Tahun 2002 tentang Hak Cipta
Undang-undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik
Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
Putusan Mahkamah Agung Nomor : 022 K/N/HaKI/2006